

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157223

(43)Date of publication of application : 31.05.2002

(51)Int.Cl.

G06F 15/00
G06F 17/30
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 2000-355635

(71)Applicant : HITACHI LTD

(22)Date of filing : 17.11.2000

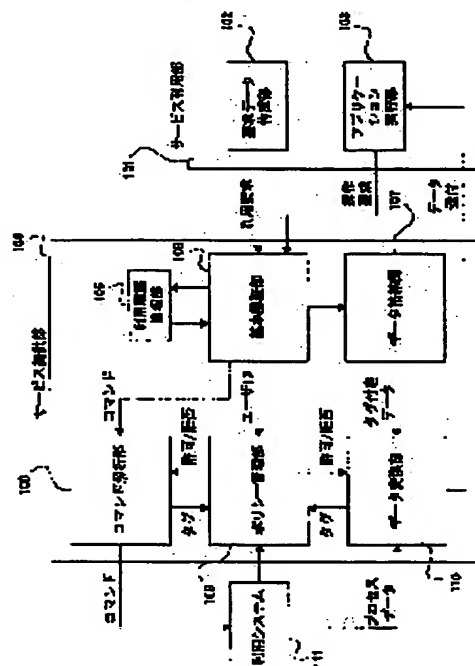
(72)Inventor : KATO HIROMITSU
FURUYA MASATOSHI
SEKOZAWA TERUJI
MIYAO TAKESHI

(54) SERVICE PROVIDING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To dynamically select information to be transmitted/received according to the authority of a user, and to prevent the same operation from being received plural times by erroneous operation.

SOLUTION: In a request data preparing part 102, service utilization request data are prepared and sent to a basic authentication part 106. In the basic authentication part 106, the user is authenticated, and in respect to a legal user, a service utilization request is accepted. Requested data are retrieved by a data storage part 107 and dispatched to a data converting part 110. The data converting part 110 inquires whether tagged data can be provided to the user or not to a policy managing part 109. Corresponding to the user ID of the user, the tag and the state of a utilization system 111, the policy managing part 109 judges permission/refusal and the data converting part 110 converts data so that data permitted by the policy managing part 109 can be disclosed and refused data can be hidden, and provides the data to an application executing part 103.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(43)公開日 平成14年5月31日(2002.5.31)

【特許請求の範囲】

【請求項1】利用者に対して所定のサービスを提供するための情報処理を実行するサービス提供システムであって、

前記サービスを提供するためのサービス情報を格納する手段と、

前記サービス内容を要求する要求情報、前記利用者の特徴を示すユーザ属性および前記利用者を認証する認証子を含む要求データを受付ける手段と、

前記ユーザ属性および前記認証子に基づいて、前記利用者を認証する手段と、

前記認証の結果に基づいて、前記サービス情報に含まれる情報に対する前記利用者のアクセス可否を決定する手段と、

前記要求情報に対応するサービス情報を、前記アクセス可能なサービス情報から検索する手段と、

検索された前記サービス情報を、決定された前記アクセス可否に適應するよう変換する手段と、

変換された前記サービス情報を提示する手段とを有することを特徴とするサービス提供システム。

【請求項2】請求項1に記載のサービス提供システムにおいて、

前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合には、2回目以降に入力された要求データの受信を抑止することを特徴とするサービス提供システム。

【請求項3】請求項2に記載のサービス提供システムにおいて、

前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合、前記利用者から複数入力することを確認することが入力された場合は、前記2回目以降に入力された要求データを受信することを特徴とするサービス提供システム。

【請求項4】請求項3に記載のサービス提供システムにおいて、

前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合には、前記利用者に対して、複数入力であることを示す情報を提示することを特徴とするサービス提供システム。よって利用可能な前記データ属性を制限する機能を有することを特徴とする請求項1乃至2に記載のサービス提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンテンツの配信およびコンテンツの利用をサービスとして提供するサービス提供システムに関し、特に、権利のあるものに適切にサービスを提供することでプライバシーの保護、コンテンツの不正利用防止を行なうサービス提供システムに関する。

【0002】

【従来の技術】インターネットに代表される情報通信技術の発展によって、ネットワークを介して音楽やゲームなどのコンテンツを配信したり、インターネットバンキングのように携帯電話や自宅のパソコンから残高照会や振込みを行なえるサービスが一般に普及してきている。ところが、サービス利用者が不特定多数となることで、サービス利用者の多様なニーズに対応するとともに、情報セキュリティ上の脅威への対策を十分に考慮していく必要がでてきた。

【0003】多様なニーズへの対応として、例えば特開2000-82039号「表示制御情報生成方法およびコンピュータ」に示されるように、様々な能力を有するクライアント端末に対して、それぞれの能力に応じたユーザインターフェースを提供するために、端末属性情報を参照してHTML等の表示制御情報を動的に生成するものがある。

【0004】また情報セキュリティを確保するための技術として、特開2000-19960号では「遠隔操作方法」を次のように記している。すなわち、操作端末から制御装置に制御信号を送信する際に、ユーザが制御信号を入力すると、次回操作権を発生し、制御装置側では制御信号と次回操作権と今回操作権を含む信号を共通鍵で暗号化し、操作端末に転送する。次回操作権は操作端末に記憶する。制御装置側では転送された暗号文を共通鍵で復号化し、制御信号と今回操作権と次回操作権とを取得し、今回操作権が制御装置側に登録してある操作権と一致するかを判定し、一致する場合は制御機器に制御信号を送る。次回操作権は制御装置側に登録される。

【0005】

【発明が解決しようとする課題】かかる従来方法においては次のような問題がある。すなわち、特開2000-82039号に関しては、コンテンツを提供する際には、クライアント端末から送信される端末属性情報に基づいて提供するコンテンツを動的に生成するが、端末を利用して閲覧している利用者がそのコンテンツを閲覧する権限があるかどうか加味されない。コンテンツが重要な機密情報を含んでいるもの、プライバシーの保護が必要なもの、会員のみに限定して提供するもの等の場合には、提供相手となるコンテンツ利用者の権限を考慮してコンテンツを生成・配信を行なう必要がある。

【0006】また、特開2000-19960号に関しては、操作端末から誤って複数回同じ操作を行なった場合、制御装置は正当な制御信号が複数回送られてきたと認識して、同じ制御を繰り返し実行してしまう可能性がある。例えば、インターネットバンキングに本手法を適用すると、振込み操作信号を誤って複数回送信してしまった場合には、それを検知することなく、必要以上に多額の振込みをしてしまうという問題があった。

【0007】本発明の目的は、利用者の権限に沿って提供する情報、受け取る情報を動的に取捨選択するサービ

サービス提供システムを提供することにある。

【0008】本発明の他の目的は、サービス利用時に誤って同じ制御信号を複数回送信してしまった場合にも、利用者の確認無しには複数回受け付けないサービス提供システムを提供することにある。

【0009】

【課題を解決するための手段】本発明は、利用者に対して所定のサービスを提供するための情報処理を実行するサービス提供システムであって、前記サービスを提供するための複数のサービス情報を格納する手段と、前記サービス内容を要求する要求情報、前記利用者の特徴を示すユーザ属性および前記利用者を認証する認証子を含む要求データを受付ける手段と、前記ユーザ属性および前記認証子に基づいて、前記利用者を認証する手段と、前記認証の結果に基づいて、前記サービス情報に含まれる情報に対する前記利用者のアクセス可否を決定する手段と、前記要求情報に対応するサービス情報を、前記アクセス可能なサービス情報から検索する手段と、検索された前記サービス情報を、決定された前記アクセス可否に適應するよう変換する手段と、変換された前記サービス情報を提示する手段とを有する。なお、変換には、アクセス可能な情報を表示可能とし、アクセス不可能な情報の表示を抑止することを含む。

【0010】また、本発明の別の形態では、同じ要求データの受信を抑止することの特徴とする。

【0011】他、以下のサービス提供システムも本発明に含まれる。ユーザ属性と認証子を添付してリクエストを作成する要求データ作成部と、ユーザ属性と認証子からユーザ認証を行なう基本認証部と、アクセス可能なデータ属性を指定するポリシー管理部と、リクエストに基づいて要求されるデータを取り出すデータ格納部と、ポリシー管理部によって指定されたデータ属性に従ってデータを再構築してユーザに提供するデータ変換部を有するサービス提供システム。

【0012】また、送達確認値と、データ属性によって特徴付けられた操作要求に、ユーザ属性と認証子を添付して送信するアプリケーション実行部と、ユーザ属性と認証子からユーザ認証を行なう基本認証部と、送達確認値が受信済みのものでないかチェックを行なう利用履歴管理部と、アクセス可能なデータ属性を指定するポリシー管理部と、操作要求を解析しポリシー管理部の判断に基づいて利用システムを操作するコマンド解析部を有するサービス提供システム。

【0013】さらに、上記のサービス提供システムそれぞれにおいて、ポリシー管理部が、ユーザ属性によって利用可能なデータ属性を制限する機能と、利用システムの状態によって利用可能なデータ属性を制限する機能を有する。

【0014】さらに、基本認証部が、送達確認値を更新する機能と、送達確認値を利用者のみが復号化できる形

で暗号化する機能を有するサービス提供システムも本発明に含まれる。

【0015】さらに、アプリケーション実行部が、基本認証部から返信された送達確認値を受信したことを確認する機能と、送達確認値を復号化して操作要求を次回送信のために保存する機能を有するサービス提供システムも本発明に含まれる。

【0016】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。本発明の実施の一形態として、プラント監視制御システムに本発明を適用した場合のブロック図を図1に示す。図1にはサービス利用部101がサービス提供部104から情報を入手する手段と、サービス利用部101が利用システム111に対して操作を行なう手段とを記載している。

【0017】サービス利用部101は、要求データ作成部102とアプリケーション実行部103からなる。要求データ作成部102は、利用者の要求をユーザID、パスワード等とともにサービス提供部106に送る。アプリケーション実行部103はサービス提供部106から渡されたデータを閲覧したり、利用システム111に対して操作を行なったりするものである。

【0018】サービス提供部104は、利用履歴管理部105、基本認証部106、データ格納部107、ポリシー管理部109、データ変換部110、コマンド解析部108からなる。利用履歴管理部105は利用者の利用履歴を管理する。基本認証部106は利用者の認証を行なう。データ格納部107はデータを格納しておき要求に応じて必要なデータを検索する。ポリシー管理部109はデータ利用を許可するか拒否するかを判断する。データ変換部110は利用者が利用可能な形にデータを変換する。コマンド解析部108は、サービス利用部101から送られた利用システム111に対する操作コマンドを解析する。

【0019】まず、サービス利用部101がサービス提供部104から情報を入手する処理フローを図2に従って説明する。サービス利用部101は、要求データ作成部102において認証情報を付与して提供して欲しいデータを指定し（ステップ201）、サービス提供部104に要求する（ステップ202）。基本認証部106でユーザ属性と認証子が正確に関連付いているかを確認し利用者の認証を行なう（ステップ203）。利用者が認証されると、基本認証部106はデータ格納部107に対してデータの検索要求を行なう（ステップ204）。データ格納部107は要求されたデータを検索する（ステップ205）。ここで、データ格納部107に格納されているデータは各データ要素を、データ属性としてタグによって特徴付けている。データ変換部110は、検索されたタグ付きデータのタグを読み取り（ステップ206）、各々のタグ付きデータを該当利用者に提供して

よいかどうかをポリシー管理部109に問い合わせる(ステップ207)。ポリシー管理部109は基本認証部106が認証したユーザIDとタグをもとにデータ提供の許可・拒否を判定する(ステップ208)。データ変換部110はポリシー管理部109の判定結果に基づき、許可するデータは開示し、拒否するデータは隠蔽する(ステップ209)。データ変換部110は、作成したデータを利用者に提供するために暗号通信を行なう(ステップ210)。暗号通信方法としてはSSL等の既存の手法を用いることができる。ここで、公開鍵暗号方式では、皆に公開できる公開鍵と、個人で秘密にしていなければならない秘密鍵をペアで使い、公開鍵で暗号化したデータは、対となる秘密鍵でないと元のデータに復号できないという性質がある。この性質を利用して、暗号通信に用いる暗号鍵を公開鍵で暗号化して渡すことによって、認証された利用者のみにデータを提供することができる。利用者の公開鍵は、信頼できる第三者機関が電子証明書を発行することによって鍵の持ち主を保証する。

【0020】各処理ステップ毎の具体的なイメージを以下に示す。要求データ作成部102の具体例を図3に示す。図3では、ユーザ属性としてユーザID301、提供して欲しいデータとして利用希望サービスリスト303から要求データ304(ここでは「ポンプとバルブ」)を選択している。利用者の秘密鍵はパスワードによって暗号化されており、これを復号化するためにパスワード302を入力する項がある。復号化された秘密鍵は、ユーザID301と要求データ304に対してデジタル署名を行なうことに用いる。「ログイン」ボタン305を押すことにより、図4のように、ユーザID301と要求データ304のセット、これのデジタル署名401と、署名に用いた秘密鍵と対になっている公開鍵の証明書402をサービス提供部104に送信し、サービス提供部104に要求する(ステップ202)。デジタル署名401を検証することによってユーザ認証を行なうことができるので、本実施の形態では認証子としてデジタル署名401を用いる。キャンセルする場合には「キャンセル」ボタン306を押す。

【0021】基本認証部106では証明書402を検証し、正しい公開鍵を取得する。公開鍵を用いてデジタル署名401をチェックして利用者の認証を行なう(ステップ203)。正当な利用者であることが確認できた場合には、基本認証部106はデータ格納部107に対して要求されたデータの検索要求を渡し(ステップ204)、ポリシー管理部109に対してユーザIDを渡す。データ格納部では渡されたデータ要求に従って該当するデータを検索する(ステップ205)。本実施例では要求データ304として「ポンプとバルブ」を渡しており、ポンプとバルブの監視制御画面に関連するファイルを検索する。検索されたファイルの具体例を図5に示

す。ファイル内のデータはタグによって特徴付けられている。

【0022】ここで、 $\langle x \rangle y \langle /x \rangle$ はデータyはタグxで特徴付けられている。この形式のデータファイルはXML(eXtensible Markup Language)という標準的な記述言語がある。図5の場合、pumpタグ501aはポンプの監視制御画面を構成する部品を内包し、監視画面を作るwatchタグ501b、ポンプ起動制御を行なうstartタグ501c、ポンプ停止制御を行なうstopタグ501dを統括している。同様に、valveタグ501eはバルブの監視制御画面を構成する部品を内包し、監視画面を作るwatchタグ501f、バルブを開く制御を行なうopentag501g、バルブを閉じる制御を行なうclosetag501hを統括している。タグ501で囲まれたデータとして本実施例では監視制御を行なうための画面構成プログラム502を置いている。

【0023】上記のタグ付きデータファイルはデータ変換部110に渡され、サービス利用部101に提示するデータを構成するための基本データとする。データ変換部110ではタグ501を読み取り(ステップ206)、該当するタグ501の付いたデータをサービス利用部101に提供してよいかどうかポリシー管理部109に問い合わせる(ステップ207)。ポリシー管理部109では、基本認証部106から渡されたユーザID301と、データ変換部110から渡されたタグ501からデータの提供に関する許可・拒否の判断を行なう(ステップ208)。

【0024】この判断を行なうためのマトリックスを図6に示す。図6ではユーザID301a~cとタグ501a~hのマトリックスとなっており、マトリックス内の○×によって許可と拒否を表現している。例えば、ユーザID301がuser Aのユーザに対してポンプの監視画面を提供することは許可されているが、停止制御画面を提供することは拒否される。マトリックス中の条件文は情報提供を許可するための条件を記す。図6の条件文601aでは、ユーザID301がuser Bのユーザに対してポンプ監視画面を提供するための条件として「IF 電源=ON」と設定している。これは、ポンプの電源がオンの場合に限り、ポンプ監視画面を提供することを表す。同様に、ユーザID301がuser Aのユーザに対してポンプ起動画面を提供するための条件として、時刻tが9:00から17:00までであることを、条件文601bにて「IF t>9:00 and t<17:00」として記述し、ユーザID301がuser Bのユーザにポンプ停止画面を提供するための条件として、ポンプの回転数が10000未満であることを、条件文601cにて「IF 回転数<10000」として記述している。

【0025】図3ではユーザID301がuser Bのユー

「ポンプとバルブ」のサービス利用要求を出しており、これに対応して図5のタグ付きデータファイルが検索されたとする。データ変換部110では、ポリシー管理部109と連携して図7の形式の変換されたファイル701を形成する。ポンプの電源がオンで、ポンプの回転数が10000未満の場合にはuser Bに対して、ポンプ監視画面、ポンプ停止画面、バルブ監視画面、バルブ閉画面の提示が許可されており、図7はWebで情報を提供する際のデータ形式であるHTMLファイルにしたものである。図7のデータを受信したサービス利用者がWebブラウザで閲覧したイメージを図8に示す。画面上には、ポンプ監視画面801、ポンプ停止画面802、バルブ監視画面803、バルブ閉画面804が表示される。一方、ポンプの電源がオフで、ポンプ回転数が10000以下の場合には、ポンプ監視画面801、ポンプ停止画面802の提供が拒否されるので、サービス利用部101が閲覧できる画面は図9のようにバルブ監視画面803およびバルブ閉画面804になる。

【0026】以上、監視制御画面を閲覧する場合について述べたが、一般の文書を閲覧する場合にも同様な処理が可能である。機密文書の閲覧要求に対して、データ格納部107からタグ付きデータファイルとして図10のような機密文書1001を検索したとする。ここで機密文書1001はsecretタグ501iで管理され、セキュリティレベルに応じてs1、s2、s3タグをそれぞれ定義する。例えば、s1タグ501jは社内秘レベル、s2タグ501kは幹部レベル、s3タグ501Lは役員レベルの機密情報として定義し、機密文書1001を構成することができる。データ変換部110はこのタグ付きデータと、ポリシー管理部109への許可・拒否の問い合わせにより提供可能なデータを再構成する。

【0027】ポリシー管理部109では、図11に示すマトリックスを用いて許可・拒否の判断を行なう。図11は、ユーザID301がuser Aの利用者はs1タグ501i付けされた社内秘データのみ閲覧可能、ユーザID301がuser Bの利用者はs3タグ501L付けされた役員データ以外は閲覧可能、ユーザID301がuser Cの利用者はすべてのデータが閲覧可能であることを示す。ここでデータ変換部110は、ユーザID301がuser Bである利用者に対してはs3タグで囲まれたデータを「****」マークに変換して閲覧不能にしている。変換されたHTMLファイルの例を図12に示す。データ変換部110から提供されたHTMLファイルは、先に述べたステップ210の暗号通信によりサービス利用者のアプリケーション実行部103に渡される。

【0028】この画面表示例を、図13に示す。ネットワーク上を流れるデータを第三者が盗聴した場合でも、暗号通信に用いる暗号鍵を復号化するための秘密鍵がなければ、図10の画面の表示を防止することが可能になる。

【0029】本実施の形態では、利用者が変わったり利用システムの状態が変わると、提供する情報も変化するところに特徴があり、機密保護、プライバシー保護を実現している。

05 【0030】次に、サービス利用部101が利用システム111に対して安全に操作を行なう方法について図14の処理フローを用いて説明する。例として図8においてポンプ停止ボタン805を押すことによって、ポンプ停止コマンドをサービス提供部104に送信する場合を
10 考える。

【0031】ポンプ停止ボタン805が押された場合、サービス提供部104とサービス利用部101で同期をとっている値とコマンドのセットを、一つのデータとしてアプリケーション実行部103は作成する（ステップ1401）。同期を取っているデータとしては時刻やカウンタなどが考えられる。

【0032】図15に示すようにコマンド1501は、タグ付きデータとする。コマンドであることはcommandタグ501mで示され、targetタグ501nがコマンドの送信先、pumpタグ501aおよびstopタグ501cにより、ポンプを停止するコマンドであることを示す。「ad%f38wh!f74」は、
20 利用システム111に対して実際に送信されるべき制御信号1502で、利用システム111に依存する特別な
25 値である。

【0033】次に、タグ付きデータとしてのコマンド1501はユーザID301とカウンタ1503とともに、無作為に生成した暗号鍵を用いて暗号化され（ステップ1402）、暗号データ1504を形成する。暗号鍵はサービス提供部の公開鍵で暗号化する（ステップ1403）。暗号データ1504および暗号化された暗号鍵1505は、サービス利用部101の秘密鍵で署名される（ステップ1404）。アプリケーション実行部103では、暗号データ1504、暗号化された暗号鍵1505、署名データ1506、署名を検証するための電子証明書1507をセットにして基本認証部106に送信する（ステップ1405）。

【0034】基本認証部106では、電子証明書1507を検証してユーザの公開鍵を取得し（ステップ1406）、署名データ1503を公開鍵で検証する（ステップ1407）。基本認証部106はサービス提供部104の秘密鍵を用いて暗号化された暗号鍵1505を復号化し、暗号鍵を得る（ステップ1408）。この暗号鍵を用いて暗号データ1504を復号化し、カウンタ1503とコマンド1501を得る（ステップ1409）。基本認証部106はカウンタ1503を利用履歴管理部105に問い合わせ、既に受信済みのものでないかどうかチェックする（ステップ1410）。受信済みであれば、コマンド1501を拒否し（ステップ1411）、
45 受信済みでなければ、利用履歴管理部105に登録され
50

ている該ユーザのカウンタ1503を最新のものに更新し(ステップ1412)、コマンド1501をコマンド解析部に渡す(ステップ1413)。例えば、アプリケーション実行部103に保存されているユーザのカウンタ1503がnであった場合、カウンタ1503の値をn+1として添付する。送信されたカウンタ1503がn以下の場合には、送信データは既に受信済みであると判断して却下する。送信されたカウンタ1503がn+1であればコマンド1501を認証し、利用履歴管理部105の登録値をn+1に更新する。新規のカウンタ1503は、ユーザの公開鍵で暗号化されサービス利用部101に返信される(ステップ1414)。アプリケーション実行部103では、暗号化されたカウンタ1503を受信した場合に送達確認画面を表示し(ステップ1415)、ユーザの秘密鍵でカウンタ1503が復号化され、次のコマンド送信のために保存される(ステップ1416)。

【0035】本実施の形態では、サービス利用部101とサービス提供部104で同期している値を用いて同じコマンドの複数回の受信を防止しているところに特徴がある。インターネットを使ったシステムの場合、ネットワークの途中で盗聴したデータをそのまま送信する再送攻撃という不正アクセス技術があり、これを防止する。

【0036】また、誤って複数回ボタンを押してしまった場合にも、同じコマンドを複数受領することがなく、誤操作を防止することができる。また送信したコマンドが確実に利用システム111に送られたことも確認することができる。

【0037】コマンド解析部108における処理フローを図16に示す。コマンド解析部108は、コマンド1501のタグ501を解析し(ステップ1601)、ポリシー管理部109にタグ501の利用許可を問い合わせる(ステップ1602)。ポリシー管理部109ではユーザID301とタグ501、および利用システム111の状態に基づき許可・拒否の判断を行なう(ステップ1603)。拒否の場合には拒否である旨ユーザに通知し(ステップ1604)、許可の場合にはタグで囲まれた制御信号1502を利用システム111に送信する(ステップ1605)。

【0038】本実施の形態では、制御信号1502をタグ501で囲んで送信することによって、制御対象(例えばポンプ)の機器毎にデータフォーマットが異なる場合(例えばA社はX方式、B社はY方式など)にも、制御対象自体が同じであれば同じ方式によってアクセス制御が行なえるところに特徴がある。

【0039】

【発明の効果】以上述べたように、本発明によれば、利用者や利用システムの状態によって提供するコンテンツ自体を変化させ、機密保護、プライバシー保護を実現することができる。また、再送攻撃、誤操作を防止するこ

とができる。また、制御対象の機器毎にデータフォーマットが異なる場合にも、制御対象を同じタグで特徴付けることで同じ方式によってアクセス制御が適用可能であるところに特徴がある。

05 【図面の簡単な説明】

【図1】本発明を適用したサービス提供システムの全体構成図である。

【図2】本発明を適用したサービス利用者への情報提供処理の手続きを示すフローチャートである。

10 【図3】サービス利用部が利用者に対して提供する初期画面例である。

【図4】要求データ作成部において作成されるデータセットを示す図である。

15 【図5】データ格納部において格納されているプラント監視制御画面データの形式を示す図である。

【図6】ポリシー管理部において管理されているサービス提供を許可するか拒否するかを判断するルールを記述するマトリックスを示す図である。

20 【図7】データ変換部において変換されたプラント監視制御画面データの形式を示す図である。

【図8】データ変換部から渡されたプラント監視制御画面データを表示した画面例である。

25 【図9】ポリシー管理部において制限がかけられた場合の、データ変換部から渡されたデータを表示した画面例である。

【図10】データ格納部において格納されている機密データの形式を示す図である。

30 【図11】機密情報をどのユーザに許可するか拒否するかを判断するルールを記述するマトリックスを示す図である。

【図12】データ変換部において変換された機密データの形式を示す図である。

【図13】データ変換部から渡された機密データを表示した画面例である。

35 【図14】サービス利用部からサービス提供部にコマンドを送信する処理の手続きを示すフローチャートである。

【図15】サービス利用部からサービス提供部に送られるデータセットの模式図である。

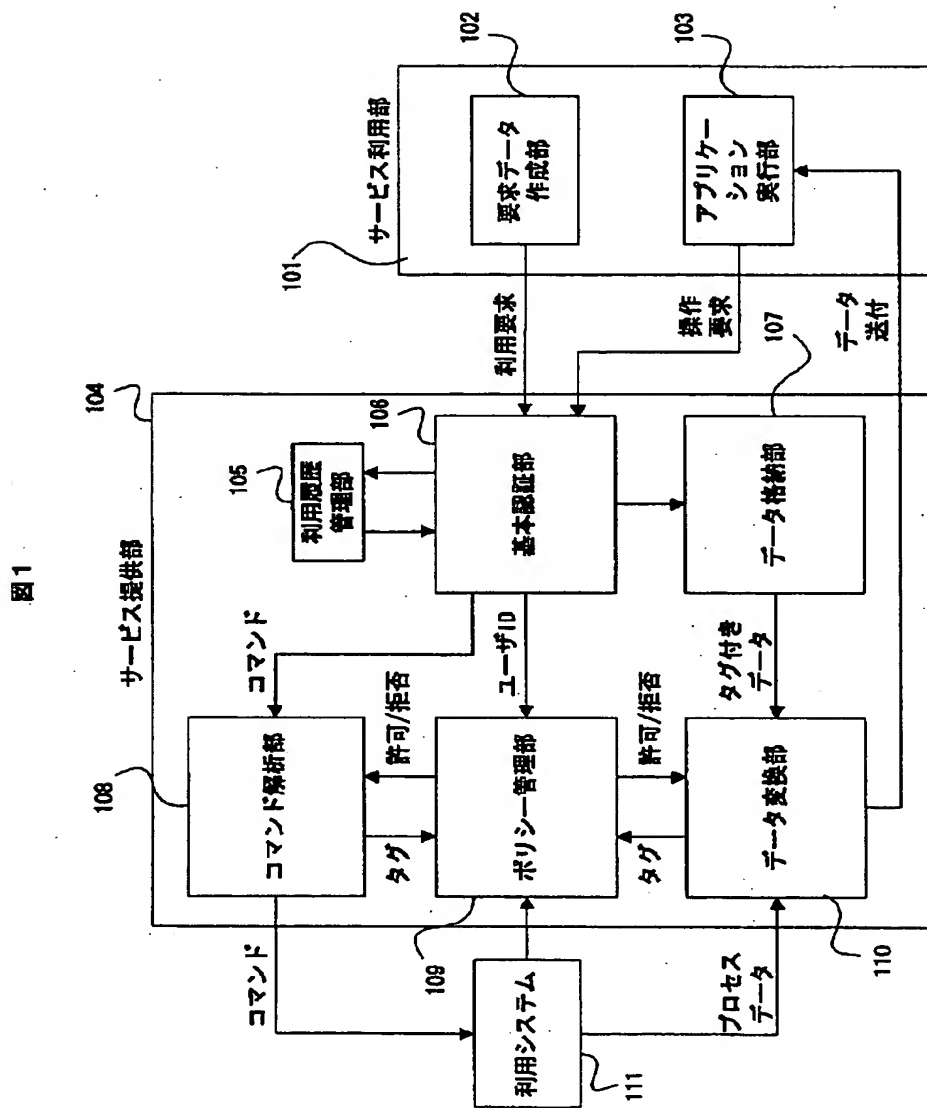
40 【図16】コマンド解析部における処理の手続きを示すフローチャートである。

【符号の説明】

301…ユーザID、302…パスワード、304…要求データ、305…ログインボタン、306…キャンセルボタン、501…タグ、502…画面構成プログラム、601…条件文、701…変換されたファイル、801…ポンプ監視画面、802…ポンプ停止画面、803…バルブ監視画面、804…バルブ閉画面、805…ポンプ停止ボタン、1501…コマンド、1502…制御信号、1503…カウンタ、1504…暗号データ

50

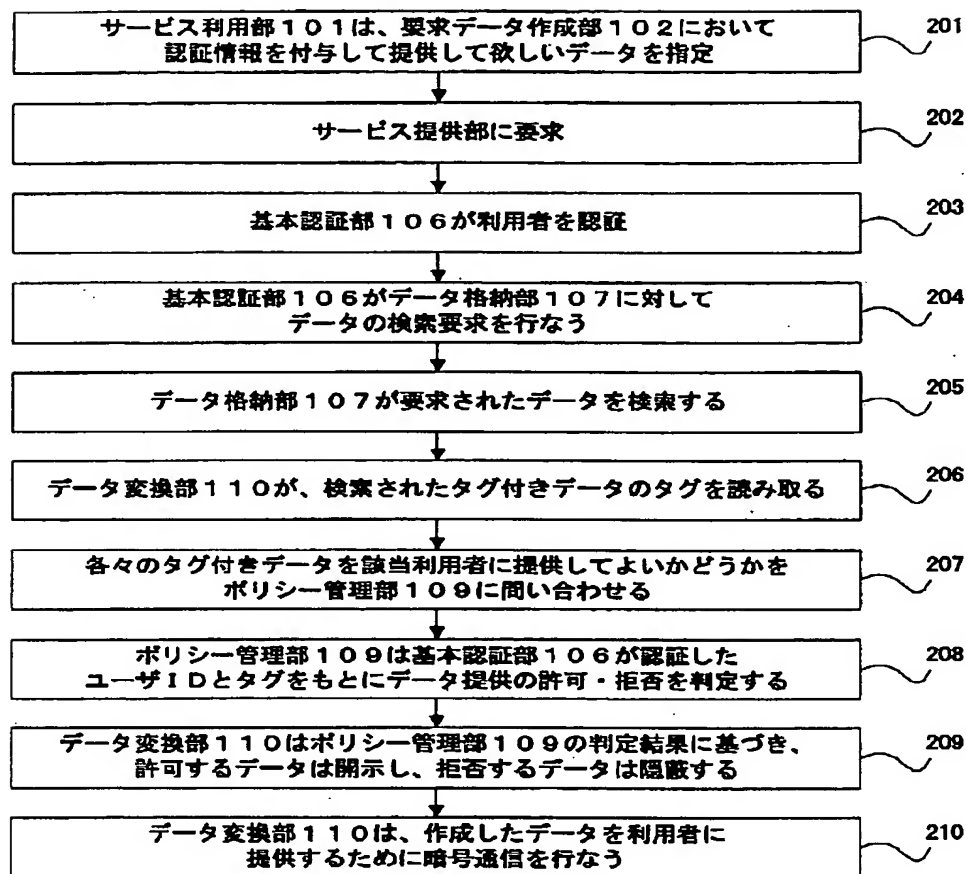
【図1】



【図2】

【図3】

図2



URL: <http://eqmweb/login/>

ユーザID

パスワード

利用希望サービス ☐ ポンプ ☒ バルブ ☐ (他) 文書閲覧

【図12】

```

<HTML>
<BODY>
  本契約における取引はA社とB社間で行われ、契約金は*****であった。
</BODY>
</HTML>
  
```

【図4】

【図5】

【図7】

ユーザID

デジタル署名

証明書

【図13】

URL: <https://eqmweb/secret/>

本契約における取引はA社とB社間で行われ、契約金は*****であった。

```

<XML Version=1.0?>
  <PUMP>
    <WATCH pump_watch.class</WATCH>
    <START pump_start.class</START>
    <STOP pump_stop.class</STOP>
  </PUMP>
  <VALVE>
    <WATCH valve_watch.class</WATCH>
    <OPEN valve_start.class</OPEN>
    <CLOSE valve_stop.class</CLOSE>
  </VALVE>
</XML>
  
```

```

<HTML>
<BODY>
  <APPLET pump_watch.class</APPLET>
  <APPLET pump_start.class</APPLET>
  <APPLET pump_stop.class</APPLET>
  <OR>
    <APPLET valve_watch.class</APPLET>
    <APPLET valve_start.class</APPLET>
    <APPLET valve_stop.class</APPLET>
  </OR>
</BODY>
</HTML>
  
```

【図10】

```

<XML Version=1.0?>
  <SECRET>
    本契約における取引はa1>A社/a1とa2>B社/a2間で行われ、契約金はa3>1,000億円/a3であった。
  </SECRET>
</XML>
  
```

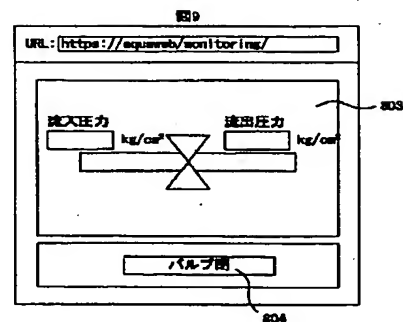
【図6】

図6

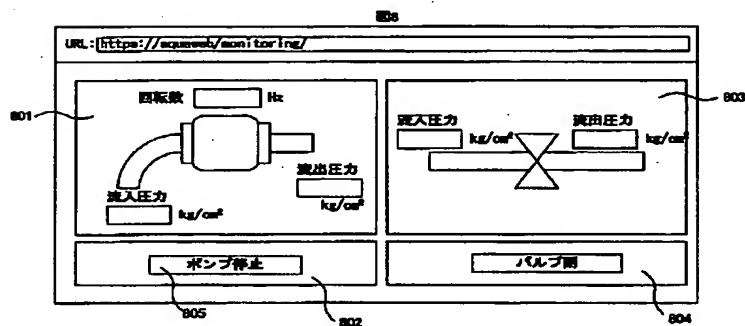
ユーザID	監視 <watch>	ポンプ <pump>	停止 <stop>	監視 <watch>	バルブ <valve>	閉 <close>
userA ~ 301a	○	IF 1 > 900 and 1 < 1700	×	○	×	×
userB ~ 301b	IF 電源 = on	×	IF 回転数 < 10000	○	×	○
userC ~ 301c	○	○	○	○	○	○

601a 601b 601c

【図9】



【図8】



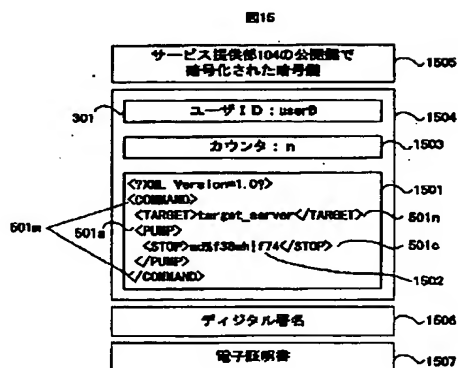
【図11】

図11

ユーザID	文書暗号<secret>	社員 <s1>	幹部 <s2>	役員 <s3>
userA ~ 301a	○	×	×	×
userB ~ 301b	○	○	○	×
userC ~ 301c	○	○	○	○

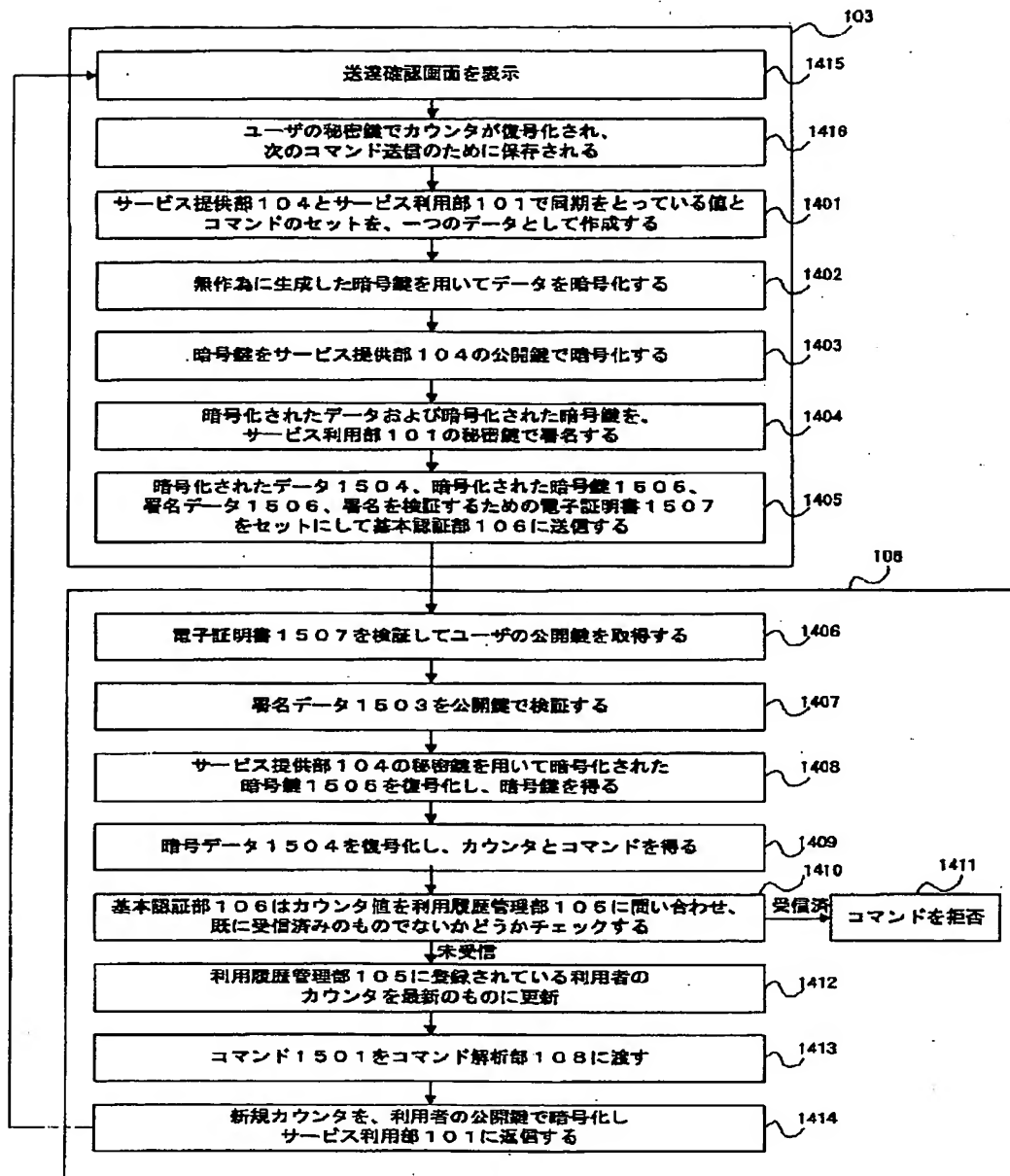
501j 501i 501k 501L

【図15】



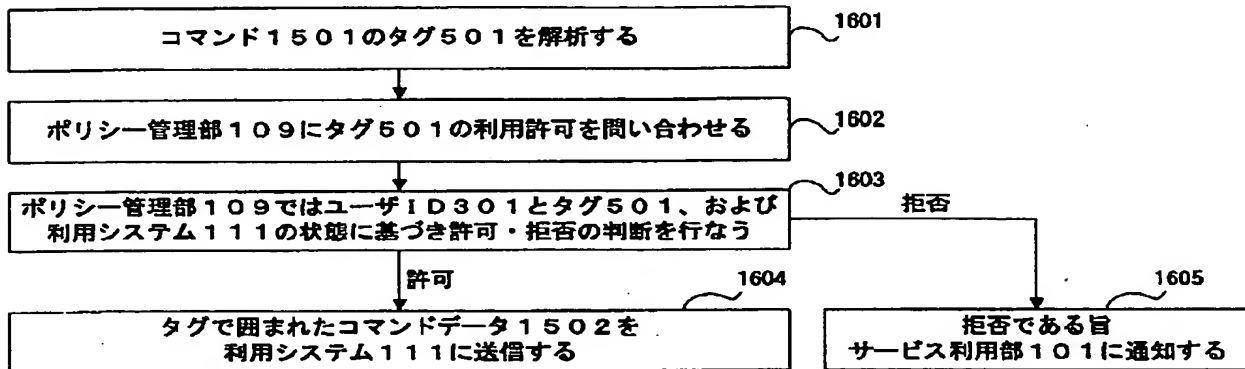
【図14】

図14



【図16】

図16



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テ-マ-ト' (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C
9/32			6 7 3 A

(72)発明者 瀬古沢 照治
 神奈川県川崎市麻生区王禅寺1099番地 株
 式会社日立製作所システム開発研究所内 30

(72)発明者 宮尾 健
 茨城県日立市大みか町五丁目2番1号 株
 式会社日立製作所情報制御システム事業部
 内

Fターム(参考) 5B075 KK54 KK63 PQ02
 5B085 AE06 AE23 BE07
 5J104 AA07 AA09 AA16 EA05 EA06
 EA19 KA01 LA03 LA06 MA02
 NA02 NA05